

- c. Ananian teaches anonymity of user profile data, without teaching any particular apparatus or method for assigning an anonymous identity, binding it uniquely and persistently to a user's real-world identity, and concealing that mapping from the server-side elements of Ananian.
- d. Turning to Ananian's drawings and detailed description for guidance, the skilled artisan would have great difficulty seeing how to implement such anonymity.

Note that Boyce, while claiming the ability to "anonymize" a user's identity (by which is meant concealment from outside parties), makes no attempt to conceal it from the service application with which he is conducting secure communications. In fact, Boyce *requires* the user to have established a prior independent relationship with the service application, details of which relationship are the basis for creating authentication credentials. Hence Boyce provides no help in achieving the kind of anonymity required by Ananian.

Ananian Fig. 2 offers no guidance in understanding where the anonymity function resides, let alone how to build it. Clearly it would have to be interposed somewhere between Actors 110 and the ICA 222 which are components of the Presentation layer 220 and embody the Actors' user interface to the Catalog Server System (CSS 200). In other references, Ananian refers to an "IDCP account" and PIN, and declares [0512] that "the CSS 200 keeps the User's identity anonymous by not merging the IDCP account number with any PII" (personally identifying information), suggesting that anonymity is conferred by the IDCP. This entity (the "Interactive Digital Catalog Profiling" network) is shown in Ananian's drawings and mentioned in his description, but is not part of the CSS 200 system for which Ananian makes his patent claims. No teaching is provided that would guide a skilled artisan in constructing that part of Ananian's concept.

- e. Ananian asserts that the CSS is "completely anonymous" ([0270]) and "does not store any personally identifiable information" ([0114]). Yet, in "another embodiment" ([0521], the CSS 2010 (synonymous with CSS 200) is described as containing an Anonymity Proxy Server 2090 (see Fig. 16), which "is configured to generate an anonymous token for each user and store the anonymous token in data store 2100 as

part of user profile 2110.” Applicant observes that generating an “anonymous token” requires access to, and retention of, a user’s real-world identity, thereby invalidating the “untrustworthy intermediary” feature underlying Thorson.

- f. In yet another alternative embodiment [0269] - [0274], Ananian applies the same teachings to “Non-anonymous networks,” describing how even anonymity may be abandoned altogether. “The CSS 200 is completely anonymous,” Ananian declares ([0270]), only to add: “However, as an alternative, the IDCP Network 100 could be configured for private networks to accommodate operation in a non-anonymous mode. This would require the ICA 222 to contain details on the User 111, and both internal and external Web services would be able to recognize and interact with the User on that basis.” Applicant observes that a system designed to accommodate both anonymous and transparent modes of access to user data hardly inspires the degree of reassurance and trust that Thorson’s patented invention would inspire in its users.

**Private key:** Thorson sequesters in quarantine memory not only user profile information, but the private key that unlocks it as well. Moreover, Thorson deletes sequestered quarantine memory contents after a subject session ends. See added claims 22 and 23. This second and third level of privacy protection is a central feature of Thorson, and there is no way that “a person having ordinary skill in the art” could learn from Boyce, or infer it therefrom by any obvious means, because the system described by Boyce does not sequester it, or suggest how such an outcome might be accomplished.

Thorson uses a two-layer encryption scheme in which the Private Key 213 needed for unlocking Encrypted PR 209 requires a second security element, the Personal Passphrase 212, which is known only to the user. Thorson does not specify how Public Key 210, Encrypted Private Key 211, and Personal Passphrase 212 are obtained, allowing that they may be “components of various encryption techniques” ([0034]), but states explicitly and unambiguously that “[a] central characteristic of all embodiments, however, is the inability of Anonymity Service 130 to access Subject’s 120 unencrypted personal data, the decryption of which requires an element kept by Subject 120 under his separate personal control and provided on request, and which cannot be duplicated or transmitted beyond the confines of Quarantine Memory 123.” This requirement absolutely precludes involvement of the Anonymity Service 130 in the creation or storage of Private Key 213 and Personal Passphrase

212, and while it allows the Anonymity Service 130 the use of Public Key 210 for encrypting its communications with Subject 120, it keeps Private Key 213 and Personal Passphrase 212 sequestered within Quarantine Memory 123 at all times.

In Boyce, by contrast, the private decryption key corresponding to the Thorson Private Key 213, required for User 12 to communicate securely with Service Applications 40, is created *at Service Provider's 20 request* by Certification Authority 14 during the registration sequence depicted from various viewpoints in Figs. 3-5. The private key is stored in a Directory 16, where it can be obtained as easily as by supplying "initialization data" likewise generated by the Service Provider 20, and stored indefinitely in Mapping Repository 26 for access whenever User 12 submits an initialization (login) request to begin a communication session.

In other words, *all the information needed for obtaining User 12's security credentials, including the private key*, remains indefinitely available to Service Provider 20. Boyce does not specify whether or how the Service Applications 40 might be denied access to the user's private key; but in any event the Service Provider 20 is clearly and ambiguously regarded as a trusted intermediary where security credentials are concerned.

For all these reasons, "someone having average skill in the art," even if he had somehow conceived Thorson's intent without prior exposure to Thorson's teachings, would find adapting Boyce to achieve that intent anything but obvious, perhaps impossible.

Applicant observes that, after removing from Boyce those elements that enable the Service Provider to create and store all the information needed for retrieval of the user's private key from its repository, and after removing all of the registration and initialization steps from Boyce's flowchart drawings (Fig. 3 Steps 70-80, Fig. 4 Steps 100-106, and Fig. 5 Steps 120-130), the skilled artisan would find little of substance remaining to learn from Boyce's teachings.

Applicant therefore asserts that Boyce is not only unhelpful in any obvious way, but in fact poses a serious and perhaps insurmountable obstacle confronting any effort to adapt the teachings of Ananian to implement Thorson's invention.

In summary, applicant asserts the following:

A. Nothing in either Boyce or Ananian or their combination anticipates or renders obvious the present invention, the focus of which is permission-based “messaging” *per se*, as opposed to the publishing of catalog content, the delivery of commercial Web services, or the transaction of online business. A “person having ordinary skill in the art” could therefore not have conceived or imagined the present invention’s claimed system, method or machine-executable medium from mere exposure to Boyce and Ananian without prior exposure to the teachings of Thorson.

B. Practitioners of secure online transactions (the province of Boyce), catalog publishing (the province of Ananian), database design and e-commerce (each a province of both Boyce and Ananian), upon encountering the present invention, would more likely have considered the present teachings and claims counterintuitive, onerous, even perverse, but nevertheless useful and advantageous, rather than “obvious,” as the Detailed Action asserts.

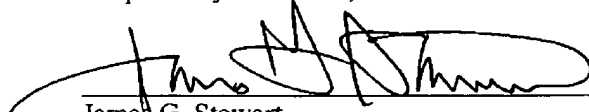
C. The way in which Boyce and Ananian are respectively organized would in fact actually *impede*, if not preclude altogether, the construction of a system with the benefit of hindsight reconstruction of the present invention.

D. If a system with the present invention’s claimed features *were* to be built using Ananian’s teachings adapted to incorporate Boyce’s, each of these systems would have to be restructured in a manner contrary to its own central underlying purpose and disclosed embodiments.

Applicant thus submits that all pending claims 1-23 are allowable.

Accordingly, applicant requests entry of the above amendment and consideration of the application on the merits. The Examiner is encouraged to telephone the undersigned at (503) 226-1191 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,



James G. Stewart  
Reg. No. 32,496  
Ater Wynne LLP  
222 SW Columbia, Suite 1800  
Portland, Oregon 97201

Customer No. 35940

I hereby certify that this correspondence  
is being transmitted to the U.S. Patent and  
Trademark Office via facsimile number  
(571) 273-8300 on November 24, 2008.



NAME